



# ISF

INFORMATION SECURITY FORUM  
FOR TEXAS GOVERNMENT

# NIST, No Mystery:

Understanding NIST SP 800-53  
and its relationship to Revised TAC 202



**Steve Caimi**

Cisco / US Public Sector Cybersecurity

# Abstract

The Revised Texas Administrative Code, Chapter 202 (TAC 202) brings the State into strategic alignment with the Federal government by adopting cybersecurity controls from NIST SP 800-53. But you might be wondering:

- Who is NIST, and what is NIST SP 800-53?
- What are the security controls and impact levels, and how are they used?
- How does 800-53 compare to the NIST Cybersecurity Framework and the NIST Risk Management Framework?
- And most importantly, how does it relate to the Revised TAC 202 Control Catalog?

In this surprisingly engaging session, we'll decrypt the NIST mystery and show how all of this works together -- to improve cybersecurity for the State of Texas.

# Agenda



1. TAC 202

2. About NIST

3. NIST SP 800-53

4. FISMA and NIST RMF

5. NIST CSF

6. Conclusion



# TAC 202

# TAC 202

## Title 1, Part 10, Chapter 202: Information Security Standards

### Subchapter B: Information Security Standards for State Agencies

- § 202.20 / Responsibilities of the Agency Head
- § 202.21 / Responsibilities of the Information Security Officer
- § 202.22 / Staff Responsibilities
- § 202.23 / Security Reporting
- § 202.24 / Agency Information Security Program
- § 202.25 / Managing Security Risks
- § 202.26 / Security Control Standards Catalog

**“ The Texas Administrative Code is a compilation of all state agency rules in Texas ”**

### Subchapter C: Information Security Standards for Institutes of Higher Education

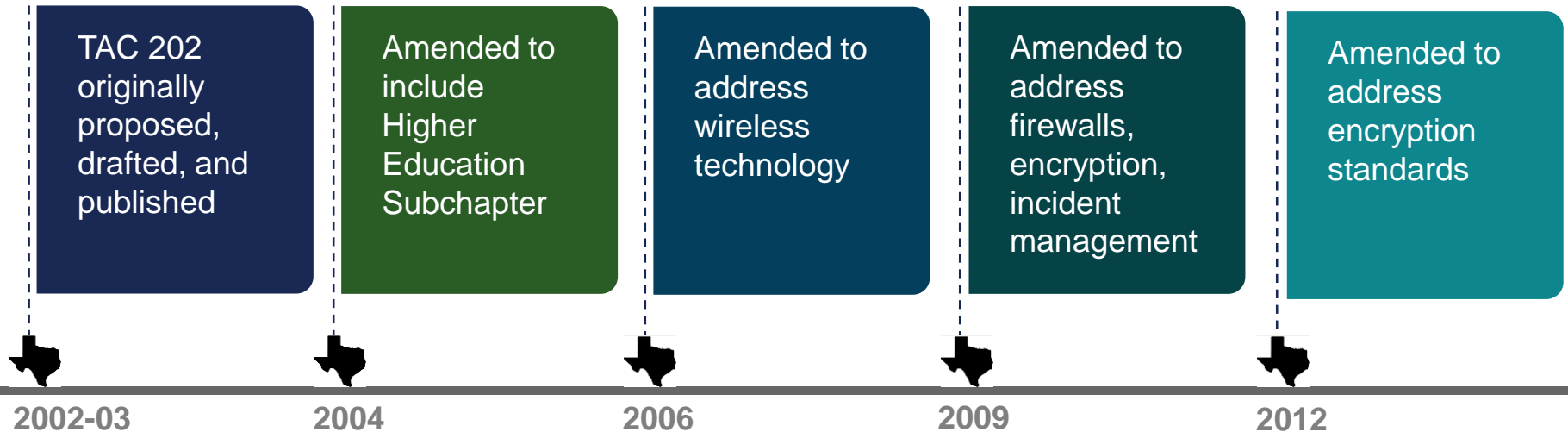
- § 202.70 / Responsibilities of the Institution Head
- § 202.71 / Responsibilities of the Information Security Officer
- § 202.72 / Staff Responsibilities
- § 202.73 / Security Reporting
- § 202.74 / Institution Information Security Program
- § 202.75 / Managing Security Risks
- § 202.76 / Security Control Standards Catalog



Dept. of Information Resources

# Legacy TAC 202

## Historical Perspective



# Legacy TAC 202

## Drivers for Change



Does not address newer technology (cloud, mobile, etc.)



Places business functions with IT (Business Continuity Planning, etc.)



Lacks many managerial and process-related controls



Creates interpretation gaps because technical controls are too vague

It's time for a Revised TAC 202

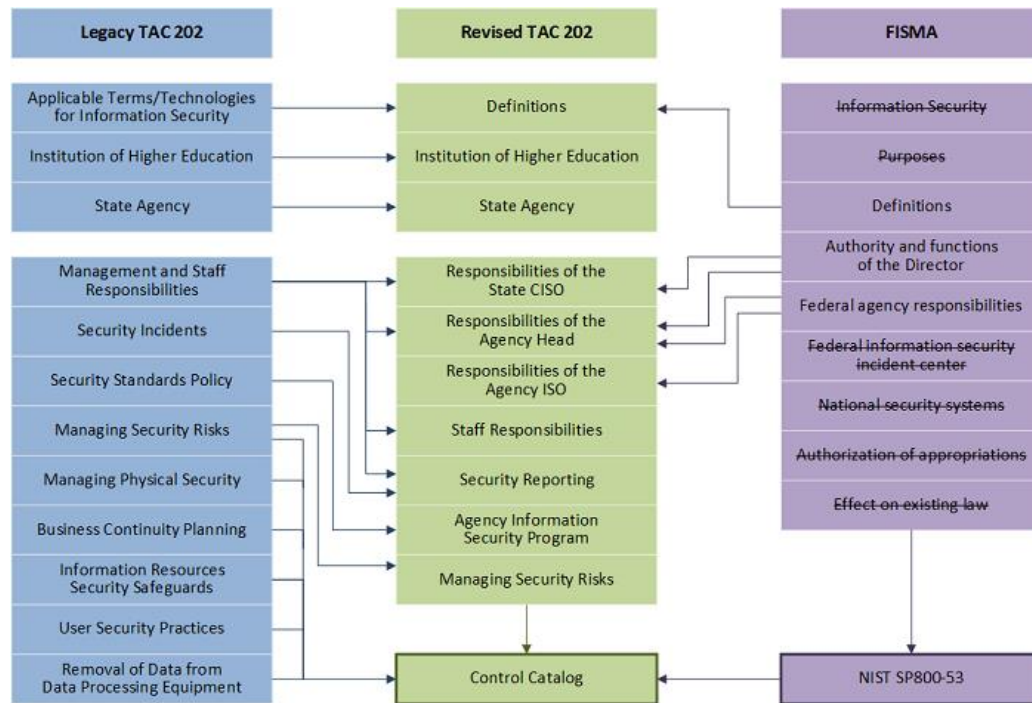




# Revised TAC 202

## Aligning with FISMA and NIST

- Committee of State ISOs revised Legacy TAC 202 for better alignment with FISMA and NIST standards
- Revised TAC 202 covers agency responsibilities and includes a Control Catalog
- Control Standards Catalog aligns with NIST SP 800-53





# Revised TAC 202

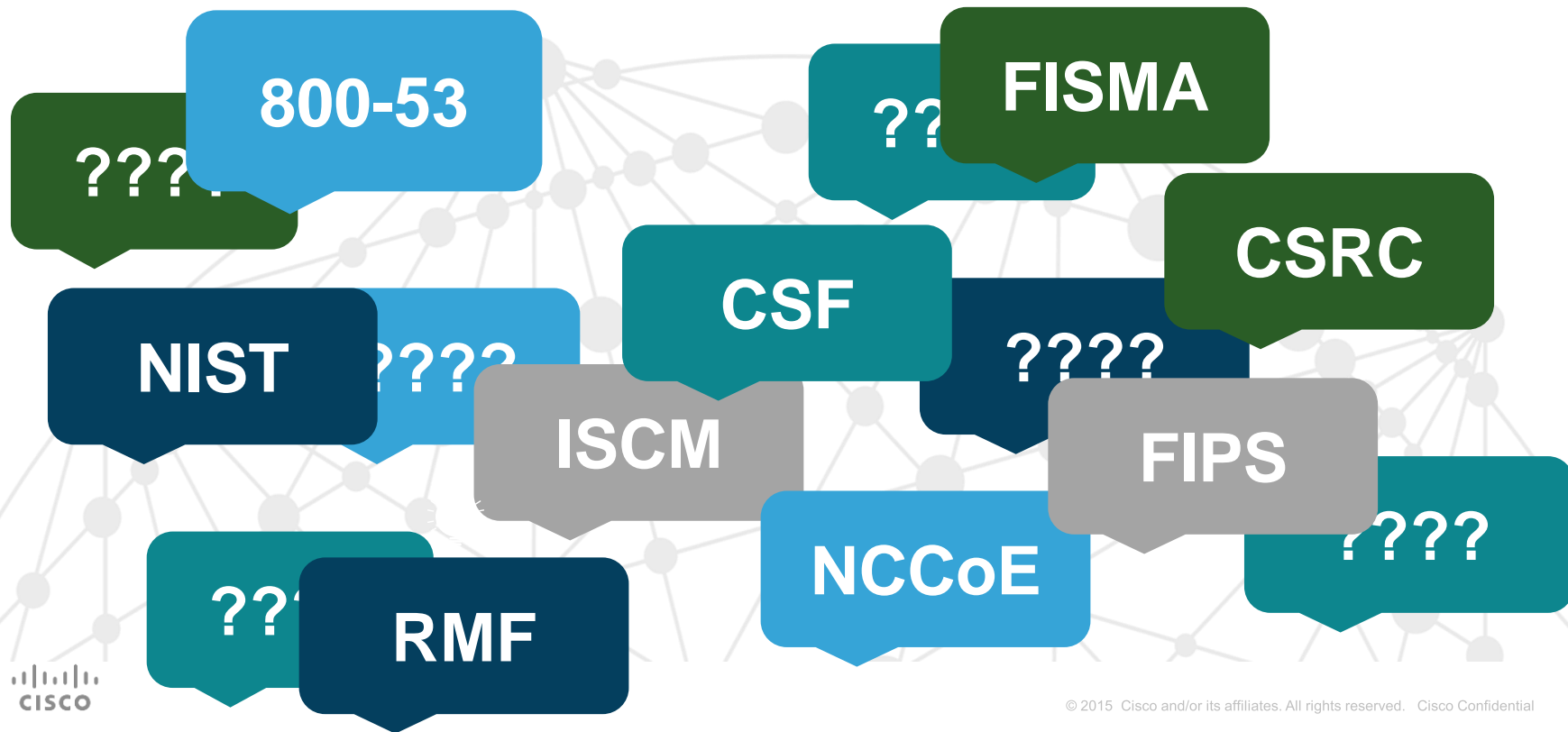
## Benefits

- Security controls separated from the state agency rules allows for **greater flexibility** and **faster updates** as technology quickly evolves
- Roles and responsibilities separated from the technical details **increases clarity** and **reduces confusion**
- Requirements clearly specified and are based on **NIST best practices** and aligns with NIST SP 800-53 nomenclature
- Control Standards Catalog still allows for **agency-specific adjustments** as needed

Group ID	AC			
Group Title	Access Control			
Control ID	AC-3			
Control Title	Access Enforcement			
Risk Statement	Misconfigured access controls provide unauthorized access to information held in application systems.			
Priority / Baseline	P1	LOW – Yes	MOD – Yes	HIGH – Yes
Required Date	February 2015			
Control Description	The organization enforces approved authorizations for logical access to the system in accordance with applicable policy.			
Implementation	State	<ol style="list-style-type: none"><li>1. Access to state information resources shall be appropriately managed.</li><li>2. Each user of information resources shall be assigned a unique identifier except for situations where risk analysis demonstrates no need for individual accountability of users. User identification shall be authenticated before the information resources system may grant that user access.</li></ol>		
Example(s)	State Organization	[to be determined]		
	Compartment	[to be determined]		
	- The organization has implemented role-based access control to determine how users may have access strictly to those functions that are described in job responsibilities.			

# Getting a bit confusing...

But we'll straighten things out!



# About NIST

### Information Technology publications, security standards, tools, and best practices

- Computer Security Resource Center (CSRC)
- Cybersecurity Framework (CSF)
- National Cybersecurity Center of Excellence (NCCoE)
- Information Technology Laboratory (ITL)
- National Strategy for Trusted Identities in Cyberspace (NSTIC)

### Breadth and depth across vast subject areas beyond Information Technology as well

- Telecommunications, nanotechnology, bioscience, energy, chemistry, math, physics, transportation, public safety -- and more



### Mission



“To promote innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life”



Federal Information Processing Standards (FIPS)



NIST Interagency or Internal Reports (NISTIRs)



Information Technology Laboratory (ITL) Bulletins



NIST Special Publications (SPs)

- **800-Series:** Computer Security
- **1800-Series:** Cybersecurity Practice Guides
- **500-Series:** Information Technology

**800-Series:** NIST's primary mode of publishing computer/cyber/information security guidelines, recommendations and reference materials.

# NIST Publications

## Key Standards and Guidelines



- **FIPS 199:** Standards for Security Categorization
- **FIPS 200:** Minimum Security Requirements
- **NIST SP 800-53:** Security and Privacy Controls
- **NIST SP 800-160:** Building Trustworthy Resilient Systems (Draft)
- **NIST SP 800-53A:** Assessing Security and Privacy Controls
- **NIST SP 800-37:** Applying the Risk Management Framework (RMF)
- **NIST SP 800-137:** Information Security Continuous Monitoring (ISCM)
- **NIST SP 800-39:** Managing Information Security Risk
- **NIST SP 800-60:** Mapping Types of Information and Information Systems to Security Categories

# NIST Publications

## Highlighting NIST SP 800-53



- FIPS 199: Standards for Security Categorization
- FIPS 200: Minimum Security Requirements
- **NIST SP 800-53: Security and Privacy Controls**
- NIST SP 800-160: Building Trustworthy Resilient Systems (Draft)
- NIST SP 800-53A: Assessing Security and Privacy Controls
- NIST SP 800-37: Applying the Risk Management Framework (RMF)
- NIST SP 800-137: Information Security Continuous Monitoring (ISCM)
- NIST SP 800-39: Managing Information Security Risk
- NIST SP 800-60: Mapping Types of Information and Information Systems to Security Categories

### Focus Area



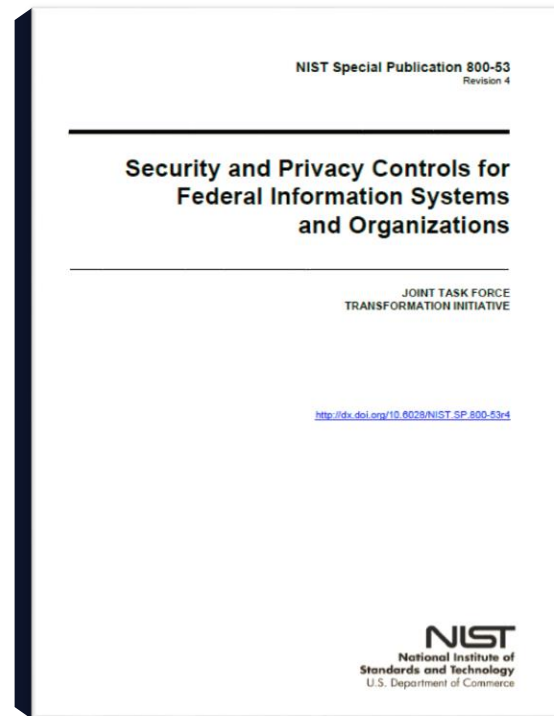
# NIST SP 800-53

### Security Control Catalog

- 18 security control families with hundreds of security controls
- Essential for FISMA and the NIST Risk Management Framework

“Special Publication 800-53, Revision 4, provides a more **holistic approach** to information security and risk management by providing organizations with the breadth and depth of security controls necessary to fundamentally strengthen their information systems and the environments in which those systems operate—contributing to systems that are more resilient in the face of cyber attacks and other threats.”

“This ‘Build It Right’ strategy is coupled with a variety of security controls for **Continuous Monitoring** to give organizations near real-time information that is essential for senior leaders making ongoing risk-based decisions affecting their critical missions and business functions.”



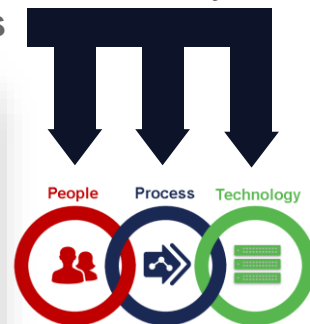
### Security Control Families

- Each family contains security controls related to the general security topic of the family
- Security controls may involve aspects of policy, oversight, supervision, manual **processes**, actions by **individuals**, or automated mechanisms implemented by **information systems/devices**

TABLE 1: SECURITY CONTROL IDENTIFIERS AND FAMILY NAMES

ID	FAMILY	ID	FAMILY
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PE	Physical and Environmental Protection
AU	Audit and Accountability	PL	Planning
CA	Security Assessment and Authorization	PS	Personnel Security
CM	Configuration Management	RA	Risk Assessment
CP	Contingency Planning	SA	System and Services Acquisition
IA	Identification and Authentication	SC	System and Communications Protection
IR	Incident Response	SI	System and Information Integrity
MA	Maintenance	PM	Program Management

A two-character ID uniquely identifies security control families



# NIST SP 800-53

## Security Control Structure

TABLE 1: SECURITY CONTROL IDENTIFIERS AND FAMILY NAMES

ID	FAMILY	ID	FAMILY
AC	Access Control	MP	Media Protection
AT	Awareness and Training	PE	Physical and Environmental Protection
AU	Audit and Accountability	PL	Planning
CA	Security Assessment and Authorization	PS	Personnel Security
CM	Configuration Management	RA	Risk Assessment
CP	Contingency Planning	SA	System and Services Acquisition
IA	Identification and Authentication	SC	System and Communications Protection
IR	Incident Response	SI	System and Information Integrity
MA	Maintenance	PM	Program Management

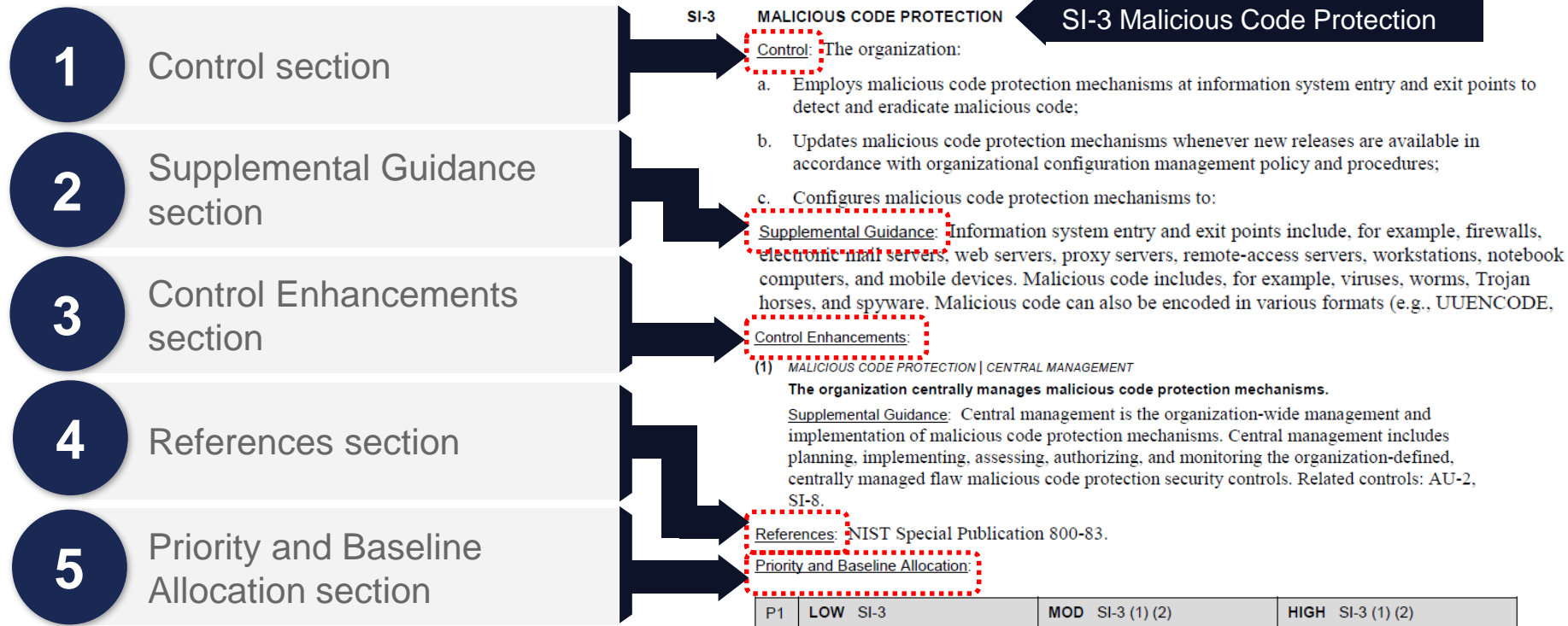
Control families drill down into individual security controls

### System and Information Integrity

SI-1	System and Information Integrity Policy and Procedures
SI-2	Flaw Remediation
SI-3	Malicious Code Protection
SI-4	Information System Monitoring
SI-5	Security Alerts, Advisories, and Directives





SI

Next slide for security control sections



# NIST SP 800-53

## Priority Codes

Priority Code	Sequencing	Action
 P1	First	Implement P1 security controls first
 P2	Next	Implement P2 security controls after implementation of P1 controls
 P3	Last	Implement P3 security controls after implementation of P1 and P2 controls
 P0	None	Security control not selected in any baseline

### System Impact Levels

#### HIGH

The loss of confidentiality, integrity, or availability could be expected to have a **severe or catastrophic adverse** effect on organizational operations, organizational assets, or individuals.

#### MOD

The loss of confidentiality, integrity, or availability could be expected to have a **serious adverse effect** on organizational operations, organizational assets, or individuals.

#### LOW

The loss of confidentiality, integrity, or availability could be expected to have a **limited adverse effect** on organizational operations, organizational assets, or individuals.

**SC = {(confidentiality, **impact**), (integrity, **impact**), (availability, **impact**)}**



# NIST SP 800-53

## Priority and Baseline Allocation

Initial Control Baselines

LOW

MOD

HIGH

SI

### System and Information Integrity

SI-1	System and Information Integrity Policy and Procedures	P1	SI-1	SI-1	SI-1
SI-2	Flaw Remediation	P1	SI-2	SI-2 (2)	SI-2 (1) (2)
SI-3	Malicious Code Protection	P1	SI-3	SI-3 (1) (2)	SI-3 (1) (2)
SI-4	Information System Monitoring	P1	SI-4	SI-4 (2) (4) (5)	SI-4 (2) (4) (5)
SI-5	Security Alerts, Advisories, and Directives	P1	SI-5	SI-5	SI-5 (1)
SI-6	Security Function Verification	P1	Not Selected	Not Selected	SI-6
SI-7	Software, Firmware, and Information Integrity	P1	Not Selected	SI-7 (1) (7)	SI-7 (1) (2) (5) (7) (14)
SI-8	Spam Protection	P2	Not Selected	SI-8 (1) (2)	SI-8 (1) (2)

Priority

# NIST SP 800-53

## Cisco Solution Alignment Summary by Control Family



		AMP/Threat Grid	Lancome StealthWatch	Cloud Access Security (CAS)	Web/Email Security	Cognitive Threat Analytics (CTA)	OpenDNS	ASA/Firepower	Identity Services Engine (ISE)	TrustSec	AnyConnect
AC	Access Control										
AT	Awareness/Training										
AU	Audit/Accountability										
CA	Security Assessment										
CM	Configuration Mgmt										
CP	Contingency Planning										
IA	Identification/AuthZ										
IR	Incident Response										
MA	Maintenance										
MP	Media Protection										
PE	Physical Environment										
PL	Planning										
PS	Personnel Security										
RA	Risk Assessment										
SA	System Acquisition										
SC	Sys/Comm Protection										
SI	Sys/Info Integrity										
PM	Program Management										

Cisco Safety  
and Security



# FISMA and NIST RMF

# FISMA

## Federal Information Security Management Act

### E-Government Act of 2002

- Recognized the importance of information security to the US economy and national security
- Established information security requirements through FISMA (Title III, Information Security)

### Federal Information Security Management Act (FISMA)

- Directed NIST to develop a new **Security Control Framework** to become the foundation of new FISMA security compliance requirements
- Requires each agency to develop, document, and implement agency-wide programs to provide information security



Public Law 107-347  
107th Congress

#### An Act

To enhance the management and promotion of electronic Government services and processes by establishing a Federal Chief Information Officer within the Office of Management and Budget, and by establishing a broad framework of measures that require using Internet-based information technology to enhance citizen access to Government information and services, and for other purposes.

Dec. 17, 2002  
[H.R. 2458]

*Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,*

E-Government  
Act of 2002.

#### SECTION 1. SHORT TITLE; TABLE OF CONTENTS.

44 USC 101 note.

(a) SHORT TITLE.—This Act may be cited as the “E-Government Act of 2002”.

(b) TABLE OF CONTENTS.—The table of contents for this Act is as follows:

- Sec. 1. Short title; table of contents.
- Sec. 2. Findings and purposes.

#### TITLE I—OFFICE OF MANAGEMENT AND BUDGET ELECTRONIC GOVERNMENT SERVICES

- Sec. 101. Management and promotion of electronic government services.
- Sec. 102. Conforming amendments.

#### TITLE II—FEDERAL MANAGEMENT AND PROMOTION OF ELECTRONIC GOVERNMENT SERVICES

- Sec. 201. Definitions.
- Sec. 202. Federal agency responsibilities.
- Sec. 203. Compatibility of executive agency methods for use and acceptance of electronic signatures.
- Sec. 204. Federal Internet portal.
- Sec. 205. Federal courts.
- Sec. 206. Regulatory agencies.
- Sec. 207. Accessibility, usability, and preservation of government information.
- Sec. 208. Privacy provisions.
- Sec. 209. Federal information technology workforce development.
- Sec. 210. Share-in-savings initiatives.
- Sec. 211. Authorization for acquisition of information technology by State and local governments through Federal supply schedules.
- Sec. 212. Integrated reporting study and pilot projects.
- Sec. 213. Community technology centers.
- Sec. 214. Enhancing crisis management through advanced information technology.
- Sec. 215. Disparities in access to the Internet.
- Sec. 216. Disparities in access to electronic information and services.

#### Title III

#### TITLE III—INFORMATION SECURITY

- Sec. 302. Management of information technology.
- Sec. 303. National Institute of Standards and Technology.
- Sec. 304. Information Security and Privacy Advisory Board.
- Sec. 305. Technical and conforming amendments.

# FISMA Objectives



C

## Confidentiality

“Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information...”



I

## Integrity

“Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity...”



A

## Availability

“Ensuring timely and reliable access to and use of information...”

# FISMA Compliance

## Security Control Framework

1 Determine Security Category

**FIPS 199**

Standards for Security Categorization of Federal Information and Information Systems

2 Apply Security Requirements

**FIPS 200**

Minimum Security Requirements for Federal Information and Information Systems

3 Select Baseline Security Controls

**NIST SP 800-53**

Security and Privacy Controls for Federal Information Systems and Organizations

Categorize Systems

Select Control Baseline

# Beyond Compliance

## Risk-Based Security Management

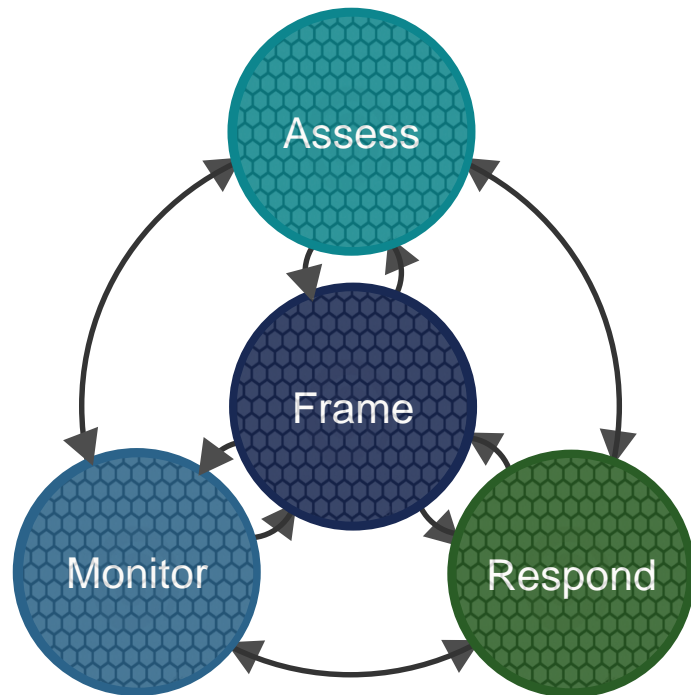
### Impossible to eliminate all cyber risks

1. **Frame:** Establish a risk context... **Security Category**
2. **Assess:** Threats, Vulnerabilities, Harm, and Likelihood
3. **Respond:** Accept, Avoid, Mitigate, Transfer, or Share
4. **Monitor:** The threat landscape changes constantly!

### Achieve “Adequate Security”

- **OMB Circular A-130:** “Security commensurate with risk resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of information”
- **Goal:** To make informed judgments and investments that mitigate risks to an acceptable level

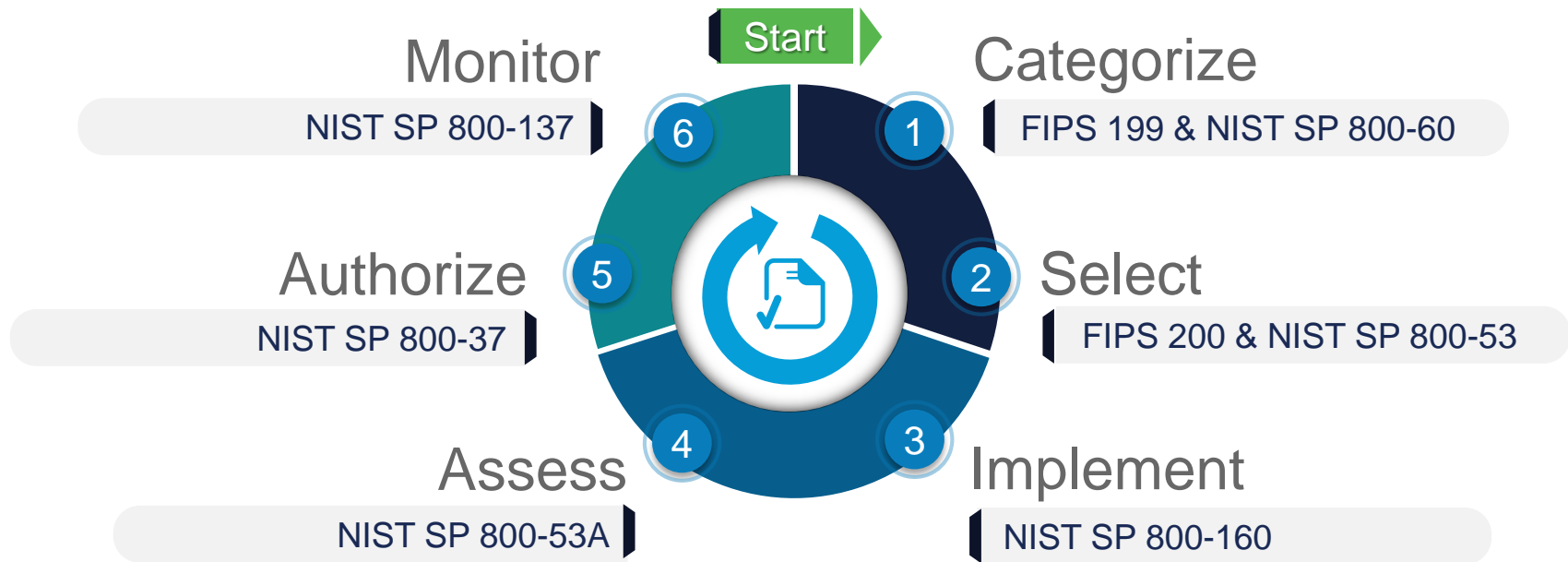
### Risk Management Process





# NIST RMF

## Risk Management Framework



# Categorize

FIPS 199 and  
NIST SP 800-60



## System Impact Levels

### High

The loss of confidentiality, integrity, or availability could be expected to have a **severe or catastrophic adverse** effect on organizational operations, organizational assets, or individuals.

### Moderate

The loss of confidentiality, integrity, or availability could be expected to have a **serious adverse effect** on organizational operations, organizational assets, or individuals.

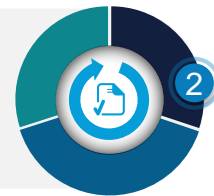
### Low

The loss of confidentiality, integrity, or availability could be expected to have a **limited adverse effect** on organizational operations, organizational assets, or individuals.

**SC** = {(confidentiality, **impact**), (integrity, **impact**), (availability, **impact**)}

# Select

FIPS 200 and  
NIST SP 800-53

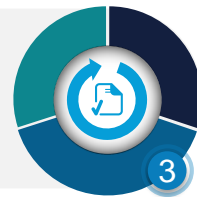


## Select the Initial Control Baseline according to System Category (SC)

CNTL NO.	CONTROL NAME	PRIORITY	INITIAL CONTROL BASELINES		
			LOW	MOD	HIGH
ACCESS CONTROL					
AC-1	Access Control Policy and Procedures	P1	AC-1	AC-1	AC-1
AC-4	Separation of Duties	P1	Not Selected	AC-4	AC-4
AC-6	Least Privilege	P1	Not Selected	AC-6(1)(2)(5)(9)(10)	AC-6(1)(2)(3)(5)(9)(10)
AC-7	Unsuccessful Logon Attempts	P2	AC-7	AC-7	AC-7
AC-11	Session Lock	P3	Not Selected	AC-11(1)	AC-11(1)

# Implement

NIST SP 800-160



**Implement the security controls and document how the controls are deployed within the information system and environment of operation**

ID	PROCESS NAME	ID	PROCESS NAME
SR	Stakeholder Requirements Definition	TR	Transition
RA	Requirements Analysis	VA	Validation
AD	Architectural Design	OP	Operation
IP	Implementation	MA	Maintenance
IN	Integration	DS	Disposal
VE	Verification		

# Assess

NIST SP 800-53A



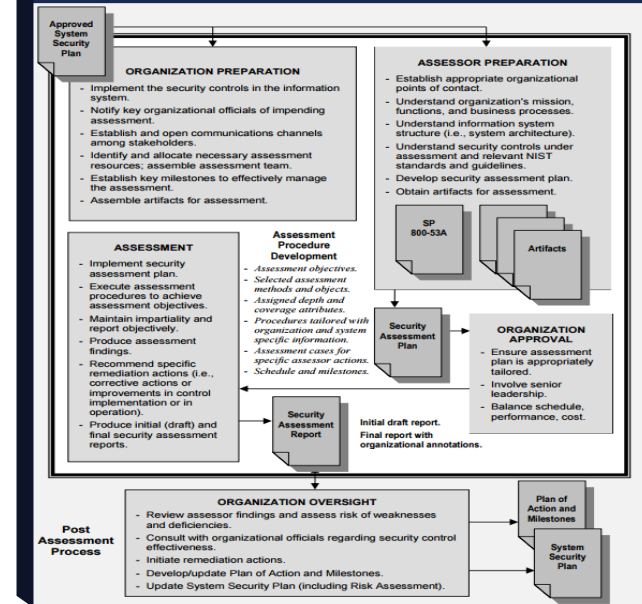
## Assess the implemented security controls to determine whether they are:

- Implemented correctly
- Operating as intended
- Producing the desired results

## Security control assessment goals:

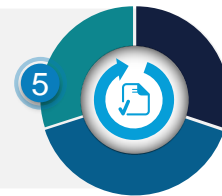
- Consistent, comparable, and repeatable assessments of security controls with reproducible results
- More cost-effective assessments of security controls
- Better understanding of the risks to organizational operations, assets, individuals

### Security Control Assessment Process Overview



# Authorize

NIST SP 800-37



1

## Plan of Action and Milestones

Prepare based on the findings and recommendations of the security assessment report excluding any remediation actions taken

2

## Security Authorization Package

Assemble the security authorization package and submit the package to the authorizing official for adjudication

3

## Risk Determination

Determine the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, etc.

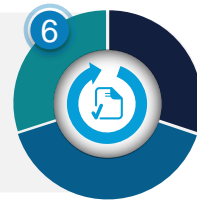
4

## Risk Acceptance

Determine if the risk to organizational operations, organizational assets, individuals, other organizations, or the Nation is acceptable

ATO

“If the authorizing official, after reviewing the authorization package deems that the risk to organizational operations and assets, individuals, other organizations, and the Nation is acceptable, an **authorization to operate** is issued for the information system or for the common controls inherited by organizational information systems”



## Information Security Continuous Monitoring (ISCM)

- Provides security situational awareness
- Enables appropriate action as the situation changes
- Part of the larger strategy of enterprise risk management

## The role of automation in ISCM

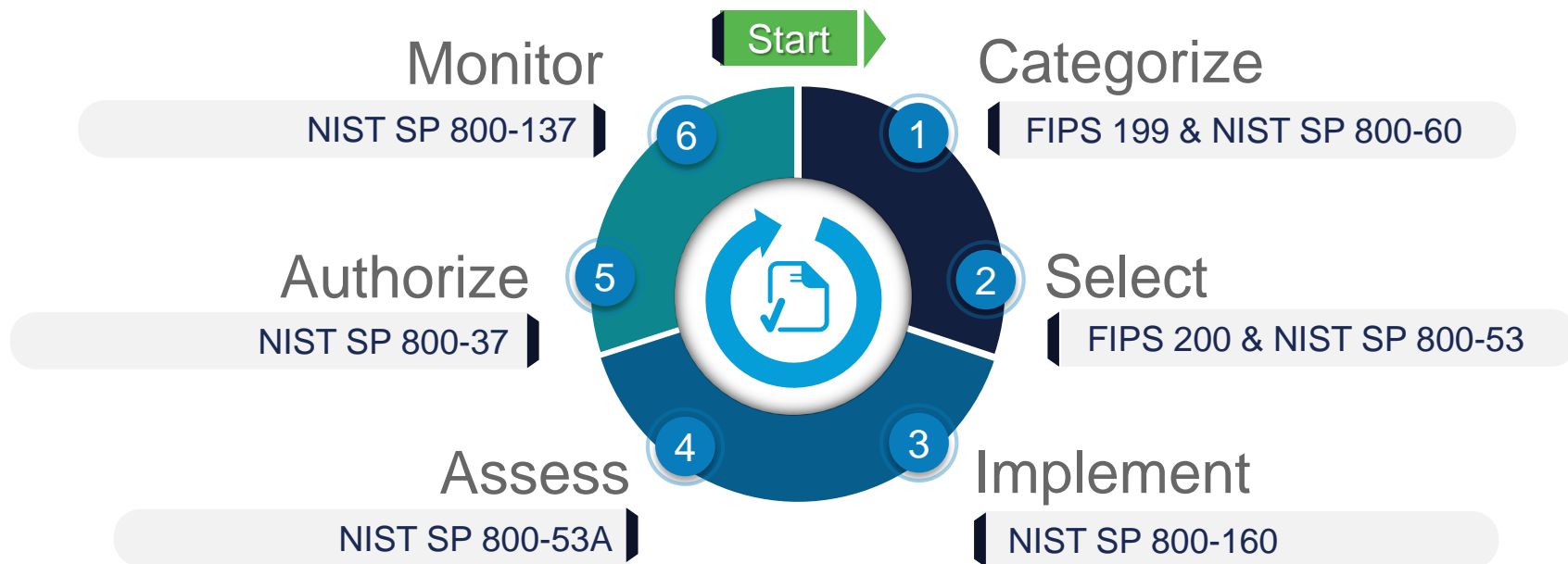
- Augments the security processes conducted by security professionals within an organization
- Reduces the amount of time a security professional must spend on doing redundant tasks
- Frees the security professional to spend time on tasks that do require human cognition





# NIST RMF Summary

## Risk Management Framework



# NIST CSF

# Improving Critical Infrastructure Cybersecurity

Executive Order 13636

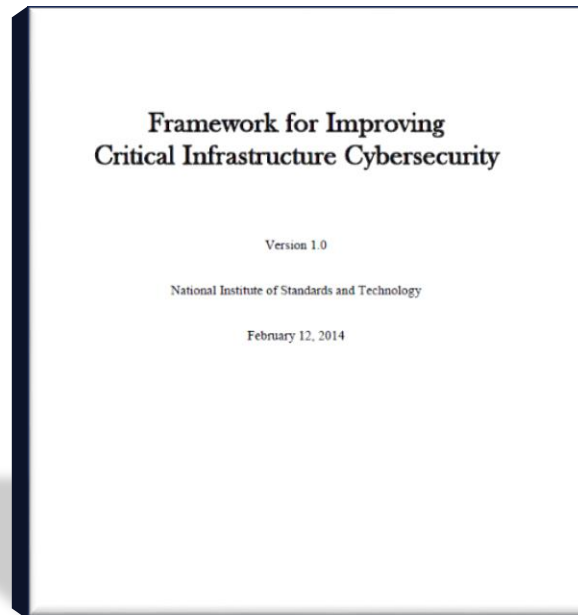
February 2013



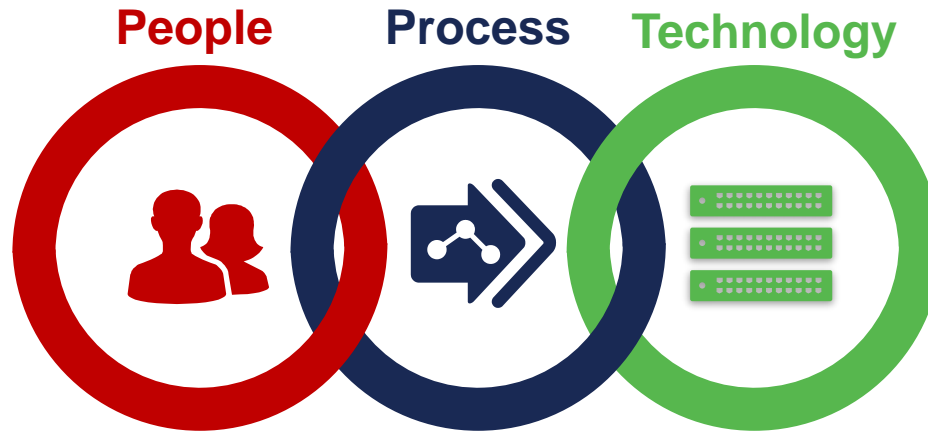
“It is the policy of the United States to enhance the security and resilience of the Nation’s critical infrastructure and to maintain a **cyber environment** that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties.”

Outcome of Executive Order 13636, and result of collaboration between public and private sectors

- Manages cybersecurity risks in a cost-effective way, while protecting privacy and civil liberties
- References the globally accepted standards (COBIT, ISO/IEC, ISA, NIST, CCS) that are working well today
- Intended for worldwide adoption -- not US only
- Uses common terminology to discuss cybersecurity risk
- Ensures business drivers guide cybersecurity activities
- Considers cybersecurity risks as part of organization's overall risk management process



# Best Practices



Framework covers all three



## Focused Action

# Framework helps organizations optimize their cybersecurity activities

- Aligns cybersecurity activities with business risk
- Prioritizes activities that are most important for critical service delivery
- Maximizes the impact of cybersecurity spending



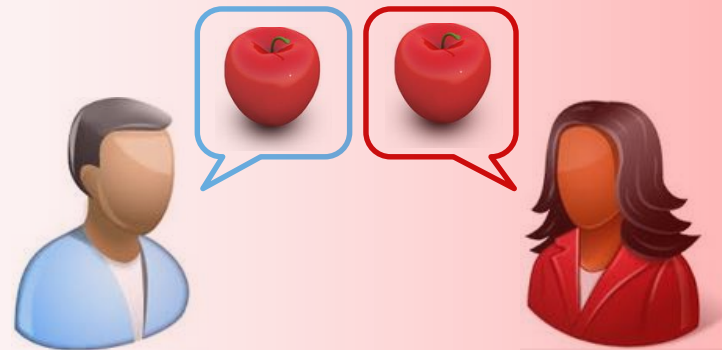
# Better Communication

People



## Framework uses a common language to discuss cybersecurity risk

- Improves communication among cybersecurity experts and senior leadership within an organization
- Improves communication with external vendors, partners, and contractors
- Aligns the Information Technology (IT) and Operations Technology (OT) teams



# Process Support



## Framework works with existing risk management programs

- ISO/IEC 27005, Information Security Risk Management
- ISO/IEC 31000, Risk Management
- NIST SP 800-39, Managing Information Security Risk
- Electricity Subsector Cybersecurity Risk Management Process (RMP)





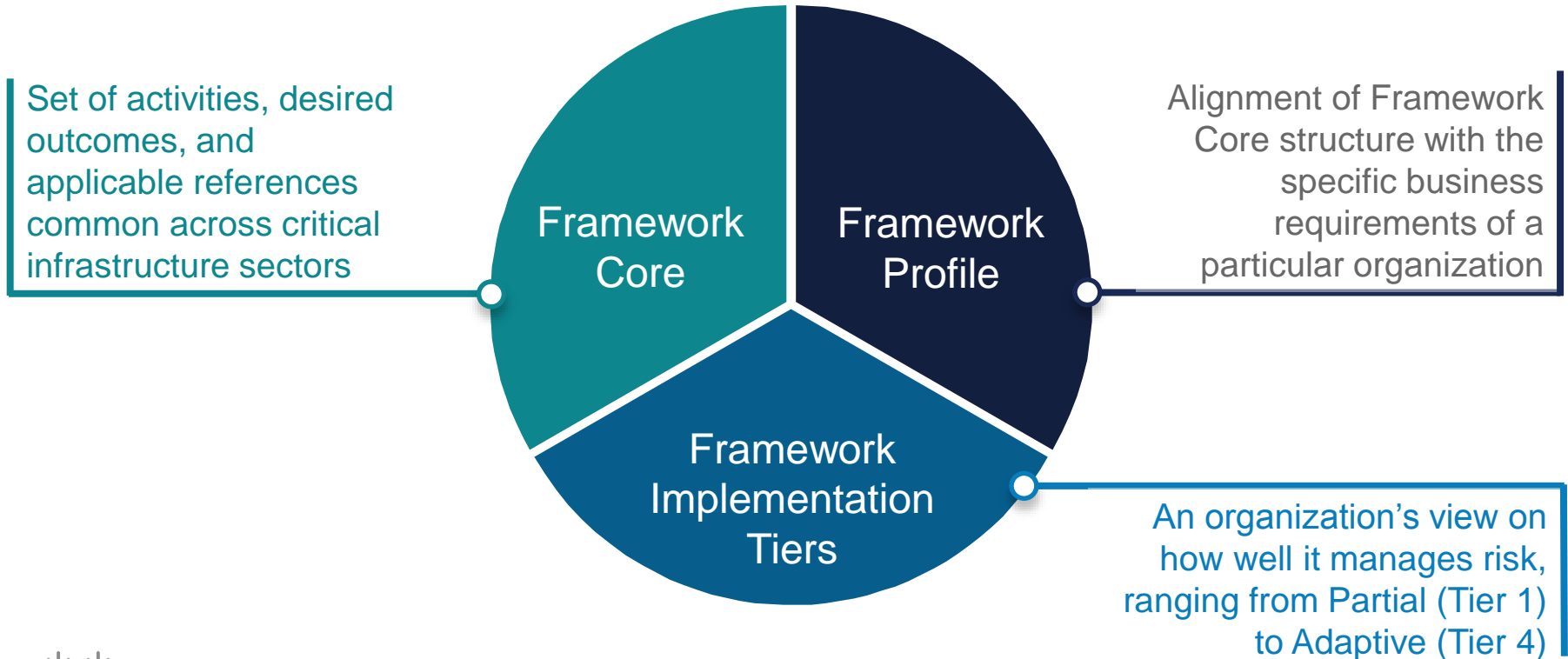
# Broad Applicability

## Framework enables all organizations to improve security and resilience

- Any size or type of organization
- Both public and private sectors
- Any degree of cybersecurity risk
- Any level of cybersecurity sophistication
- Anywhere in the world



# CSF Components



# CSF Core

Core



Functions	Categories	Subcategories	Informative Resources
Identify			
Protect			
Detect			
Respond			
Recover			

# CSF Core

Core

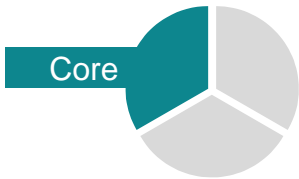


## Functions

1

High-level  
cybersecurity  
goals

CSF Core

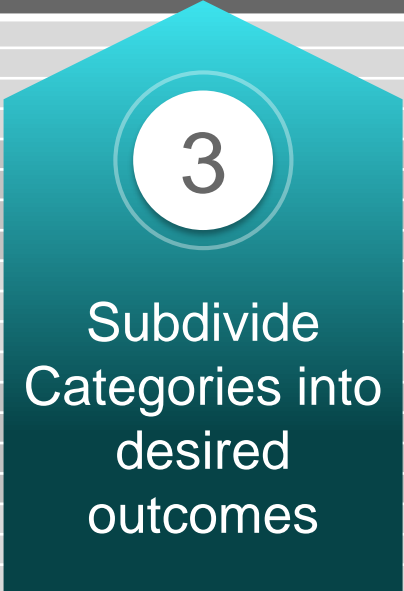


	Categories		
Identify			
Protect			
Detect			
Respond			
Recover			

# CSF Core

Core




		Subcategories	
Identify			
Protect			
Detect			
Respond			
Recover			

# CSF Core

Core



			Informative Resources
Identify			
Protect			
Detect			
Respond			
Recover			

# Functions

Core



## Functions

ID	Identify	Develop the <b>organizational understanding</b> to manage cybersecurity risk to systems, assets, data, and capabilities
PR	Protect	Develop and implement the <b>appropriate safeguards</b> to ensure delivery of critical infrastructure services
DE	Detect	Develop and implement the appropriate activities to <b>identify the occurrence</b> of a cybersecurity event
RS	Respond	Develop and implement the appropriate activities to <b>take action</b> regarding a <b>detected</b> cybersecurity event
RC	Recover	Develop and implement the appropriate activities to <b>maintain plans for resilience</b> and to <b>restore any capabilities or services</b> that were impaired due to a cybersecurity event



# Categories

Core

Function	Categories		
Identify (ID)	ID.AM	<b>Asset Management (AM)</b>	The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are <b>identified</b> and <b>managed</b> consistent with their <b>relative importance</b> to business objectives and the organization's risk strategy.
	ID.BE	<b>Business Environment (BE)</b>	The organization's <b>mission</b> , <b>objectives</b> , <b>stakeholders</b> , and <b>activities</b> are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.
	ID.GV	<b>Governance (GV)</b>	The <b>policies</b> , <b>procedures</b> , and <b>processes</b> to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cyber risk.
	ID.RA	<b>Risk Assessment (RA)</b>	The organization <b>understands the cybersecurity risk</b> to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.
	ID.RM	<b>Risk Management Strategy (RM)</b>	The organization's priorities, constraints, risk tolerances, and assumptions are established and used to <b>support operational risk decisions</b> .

# Subcategories

Core

Function	Category	Subcategories	
Identify (ID)	Asset Management (ID.AM)	ID.AM-1	<b>Physical devices and systems</b> within the organization are <b>inventoried</b>
		ID.AM-2	<b>Software platforms and applications</b> within the organization are <b>inventoried</b>
		ID.AM-3	Organizational <b>communication</b> and <b>data flows</b> are <b>mapped</b>
		ID.AM-4	<b>External information systems</b> are <b>catalogued</b>
		ID.AM-5	<b>Resources</b> (hardware, devices, data, and software) are prioritized based on their <b>classification</b> , <b>criticality</b> , and <b>business value</b>
		ID.AM-6	Cybersecurity <b>roles and responsibilities</b> for the entire workforce and third-party stakeholders (suppliers, customers, partners) are <b>established</b>

# Informative Resources

Core

Function	Category	Subcategory	Informative Resources
Identify (ID)	Asset Management (ID.AM)	Physical device inventories (ID.AM-1)	<ul style="list-style-type: none"><li>• <b>CCS CSC 1</b></li><li>• <b>COBIT 5 BAI09.01, BAI09.02</b></li><li>• <b>ISA 62443-2-1:2009 4.2.3.4</b></li><li>• <b>ISA 62443-3-3:2013 SR 7.8</b></li><li>• <b>ISO/IEC 27001:2013 A.8.1.1, A.8.1.2</b></li><li>• <b>NIST SP 800-53 Rev. 4 CM-8</b></li></ul>

## International standards references

- Council on CyberSecurity (CCS)
- Control Objectives for Information and Related Technology (COBIT)
- International Society of Automation (ISA)
- International Organization for Standardization (ISO)
- International Electrotechnical Commission (IEC)

# Informative Resources

Core

Function	Category	Subcategory	Informative Resources
Identify (ID)	Asset Management (ID.AM)	Physical device inventories (ID.AM-1)	<ul style="list-style-type: none"> <li>• CCS CSC 1</li> <li>• COBIT 5 BAI09.01, BAI09.02</li> <li>• ISA 62443-2-1:2009 4.2.3.4</li> <li>• ISA 62443-3-3:2013 SR 7.8</li> <li>• <b>ISO/IEC 27001:2013 A.8.1.1, A.8.1.2</b></li> <li>• NIST SP 800-53 Rev. 4 CM-8</li> </ul>



ISO/IEC 27001:2013 Annex A	
A.8 Asset Management	
A.8.1.1	Inventory of Assets
A.8.1.2	Ownership of Assets

# Tiers



Reflect how an organization views cybersecurity risk and the processes in place to manage that risk

- Tier 4 › **Adaptive**: Practices fully established and continuously improved
- Tier 3 › **Repeatable**: Practices approved and established by organizational policy
- Tier 2 › **Risk Informed**: Practices approved but not completely established by policy
- Tier 1 › **Partial**: Informal, ad hoc, reactive responses

The alignment of the Framework core with an organizations business requirements, risk tolerance, and resources

- Describes the current state and desired future state
- Reveals gaps that can flow into action plan development
- Facilitates a roadmap for reducing cybersecurity risk



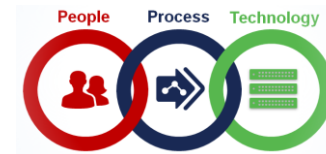
# High Level Core View

Core

Function		Category	
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
DE	Detect	PR.PT	Protective Technology
		DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
RS	Respond	DE.DP	Detection Processes
		RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
RC	Recover	RS.IM	Improvements
		RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

- ◀ Know what you have
- ◀ Secure what you have
- ◀ Spot threats quickly
- ◀ Take action immediately
- ◀ Restore operations

# Important Points



Function		Category		People	Process	Technology
ID	Identify	ID.AM	Asset Management	Applies	Applies	Applies
		ID.BE	Business Environment	Applies	Applies	
		ID.GV	Governance	Applies	Applies	
		ID.RA	Risk Assessment	Applies	Applies	Applies
		ID.RM	Risk Management Strategy	Applies	Applies	
PR	Protect	PR.AC	Access Control	Applies	Applies	Applies
		PR.AT	Awareness and Training	Applies	Applies	
		PR.DS	Data Security	Applies	Applies	Applies
		PR.IP	Information Protection Processes and Procedures	Applies	Applies	Applies
		PR.MA	Maintenance	Applies	Applies	Applies
		PR.PT	Protective Technology	Applies	Applies	Applies
DE	Detect	DE.AE	Anomalies and Events	Applies	Applies	Applies
		DE.CM	Security Continuous Monitoring	Applies	Applies	Applies
		DE.DP	Detection Processes	Applies	Applies	
RS	Respond	RS.RP	Response Planning	Applies	Applies	
		RS.CO	Communications	Applies	Applies	
		RS.AN	Analysis	Applies	Applies	Applies
		RS.MI	Mitigation	Applies	Applies	Applies
		RS.IM	Improvements	Applies	Applies	
RC	Recover	RC.RP	Recovery Planning	Applies	Applies	
		RC.IM	Improvements	Applies	Applies	
		RC.CO	Communications	Applies	Applies	

Only half of the Framework's Categories are addressed by **technology**

Highlights the importance of both **people** and **process** in cybersecurity



# CSF Uses

Basic  
Review  
of  
Cybersecurity  
Practices



“How well are  
we doing  
today?”

Establishing  
or Improving  
a  
Cybersecurity  
Program



“Can we  
assess and  
improve?”

Let's focus here

Communicating  
Cybersecurity  
Requirements  
with  
Stakeholders



“Can we speak  
the same  
language?”

Identifying  
Opportunities  
for Updated  
Informative  
References



“What else  
should we  
consider?”

Methodology  
to  
Protect Privacy  
and  
Civil Liberties



“Can we  
protect data  
better?”

# Improving a Program

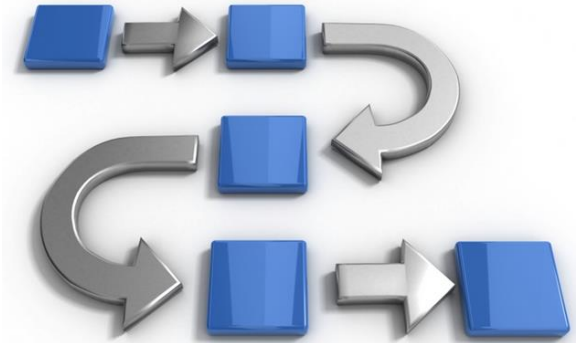


# Prioritize and Scope



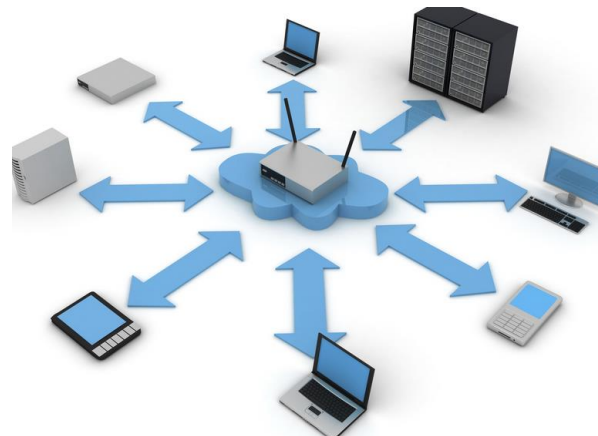
## Identify business/mission objectives and high-level organizational priorities

- Make strategic decisions on cybersecurity
- Determine scope of systems and assets that support the mission
- Assess risk tolerance

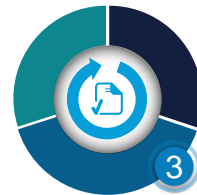


## Identify related systems, regulatory requirements, and overall risk approach

- Identify threats to systems and assets
- Identify vulnerabilities associated with systems and assets



# Current Profile



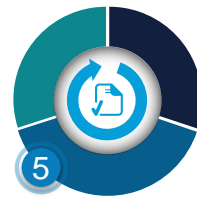
Function	Category	Subcategory	Current Profile	
Identify (ID)	Asset Management (ID.AM)	Physical device inventories (ID.AM-1)	Tier 1	Manual, spreadsheet-based system is insufficient and lacks network visibility.
		Software inventories (ID.AM-2)	Tier 1	Asset management system cannot detect new software applications being deployed.
		Communication/data flow maps (ID.AM-3)	Tier 2	Flow maps are documented and approved but needs to be formalized by policy.
		External system catalogs (ID.AM-4)	Unused	Current business model does not require external system catalogs.
		Resource prioritization (ID.AM-5)	Tier 4	Prioritization system is working well for our needs today.
		Roles/responsibilities clarification (ID.AM-6)	Tier 3	New cybersecurity responsibilities need to be formalized by policy.

# Risk Assessment



Fxn.	Cat.	Sub.	Current Profile	Risk Assessment	
ID	ID.AM	ID.AM-1	Tier 1	✗	Unacceptably high risks
		ID.AM-2	Tier 1	✗	
		ID.AM-3	Tier 2	✓	Acceptable risks at this time
		ID.AM-4	Unused	✓	
		ID.AM-5	Tier 4	✓	
		ID.AM-6	Tier 3	✓	

# Target Profile

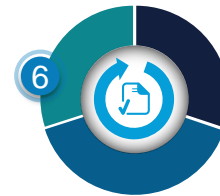


This is where we want to be ➔

- Physical device and software inventories at Tier 4, “Adaptive”
- Practices fully established, continuously improved, and built into our overall risk management program

Fxn.	Cat.	Sub.	Target Profile
ID	ID.AM	ID.AM-1	Tier 4
		ID.AM-2	Tier 4
		ID.AM-3	Tier 2
		ID.AM-4	Unused
		ID.AM-5	Tier 4
		ID.AM-6	Tier 3

# Gap Analysis



Fxn.	Cat.	Sub.	Current Profile
ID	ID.AM	ID.AM-1	Tier 1
		ID.AM-2	Tier 1
		ID.AM-3	Tier 2
		ID.AM-4	Unused
		ID.AM-5	Tier 4
		ID.AM-6	Tier 3

Enables a  
**prioritized**  
action plan

Fxn.	Cat.	Sub.	Target Profile
ID	ID.AM	ID.AM-1	Tier 4
		ID.AM-2	Tier 4
		ID.AM-3	Tier 2
		ID.AM-4	Unused
		ID.AM-5	Tier 4
		ID.AM-6	Tier 3



# Action Plan



Fxn.	Cat.	Sub.	Informative Resources
ID	ID.AM	ID.AM-1	<ul style="list-style-type: none"> <li>CCS CSC 1</li> <li>COBIT 5 BAI09.01, BAI09.02</li> <li>ISA 62443-2-1:2009 4.2.3.4</li> <li>ISA 62443-3-3:2013 SR 7.8</li> <li>ISO/IEC 27001:2013 A.8.1.1, A.8.1.2</li> <li><b>NIST SP 800-53 Rev. 4 CM-8</b></li> </ul>
		ID.AM-2	<ul style="list-style-type: none"> <li>CCS CSC 2</li> <li>COBIT 5 BAI09.01, BAI09.02, BAI09.05</li> <li>ISA 62443-2-1:2009 4.2.3.4</li> <li>ISA 62443-3-3:2013 SR 7.8</li> <li>ISO/IEC 27001:2013 A.8.1.1, A.8.1.2</li> <li><b>NIST SP 800-53 Rev. 4 CM-8</b></li> </ul>

## NIST SP 800-53 Revision 4

### **CM-8 / Information System Component Inventory**

Control: The organization:

a. Develops and documents an inventory of information system components that:

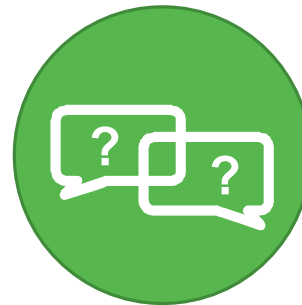
1. Accurately reflects the current information system;
2. Includes all components within the authorization boundary of the information system;
3. Is at the level of granularity deemed necessary for tracking and reporting; and
4. Includes [*Assignment: organization-defined information deemed necessary to achieve effective information system component accountability*]

# Develop Action Plan

## Device Inventory



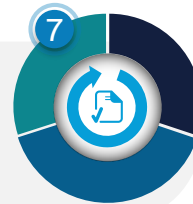
We need an accurate device inventory...



...but how can we know what's actually on our network?

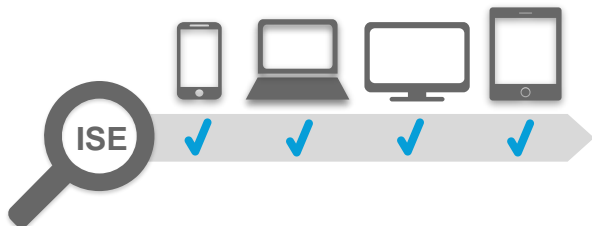
# Implement Action Plan

## Device Discovery and Profiling



## Cisco Identity Services Engine (ISE)

- Discovers and accurately identifies devices connected to wired, wireless, and virtual private networks



### NIST SP 800-53 Revision 4

#### CM-8 / Information System Component Inventory

Control: The organization:

a. Develops and documents an inventory of information system components that:

1. Accurately reflects the current information system;
2. Includes all components within the authorization boundary of the information system;
3. Is at the level of granularity deemed necessary for tracking and reporting; and
4. Includes [*Assignment: organization-defined information deemed necessary to achieve effective information system component accountability*]

# Continuous Improvement

Not once and done!

Implement Action Plan

Prioritize and Scope

Analyze Gaps

Orient

Create Target Profile

Create Current Profile

Conduct Risk Assessment



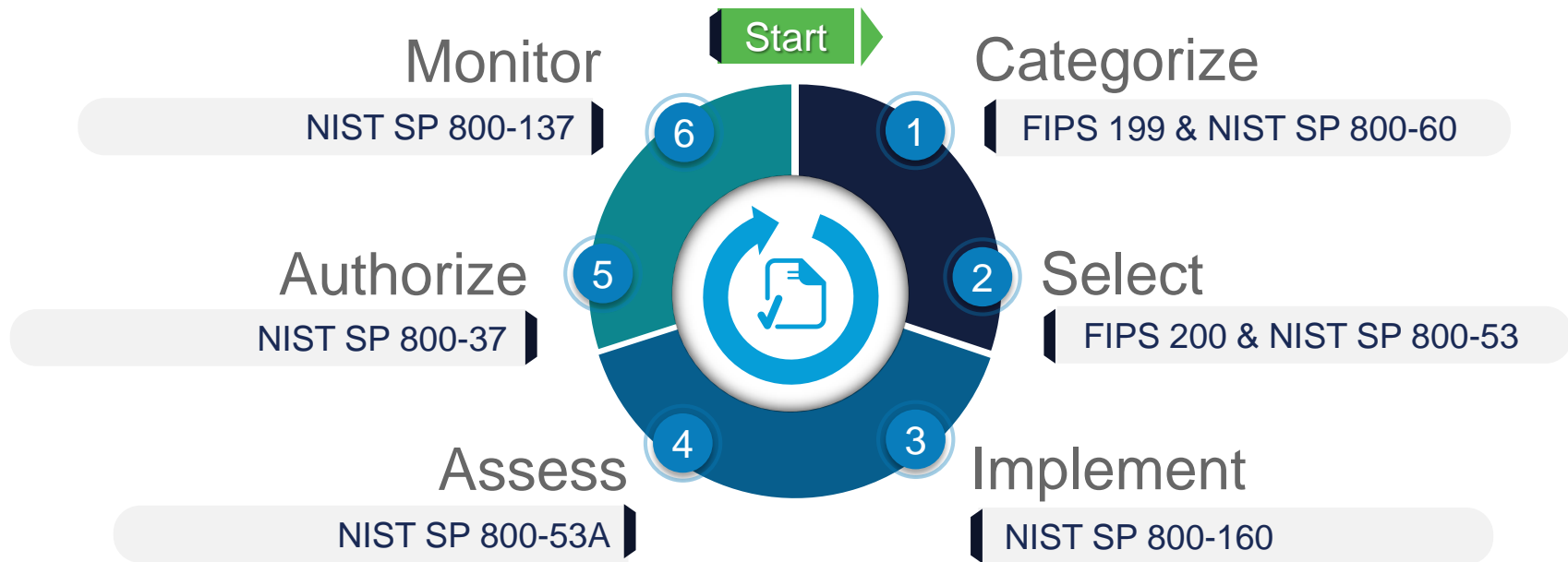
# NIST RMF vs. NIST CSF

What's the difference?



# NIST RMF Overview

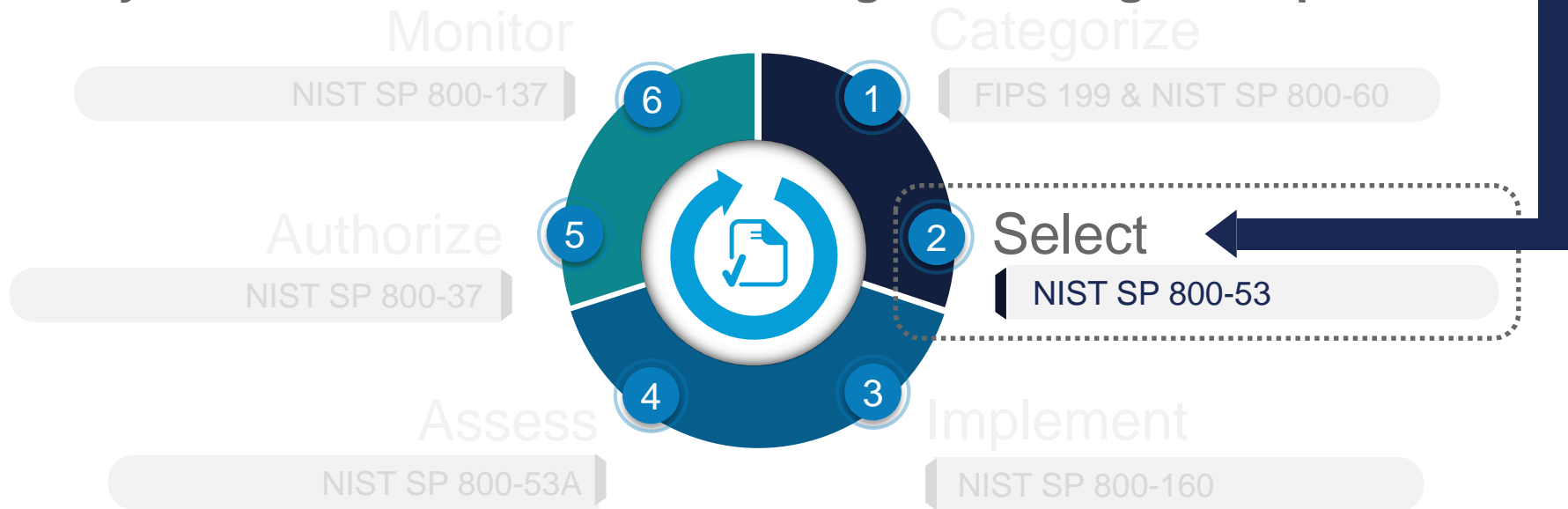
## Risk Management Framework



# NIST RMF vs. NIST CSF

## Security Control Selection

NIST CSF guides organizations to risk-based **Selection** of effective security controls for inclusion in existing risk-management process



# NIST RMF vs. NIST CSF

## Other Important Differences

### **NIST CSF can be used with the NIST RMF but does not require it**

- Organizations may choose to follow the NIST RMF, but are also free choose to use the NIST CSF with ISO/IEC 27005 -- or any other enterprise risk management process

### **NIST CSF references the NIST SP 800-53 security control catalog but does not require it**

- Organizations may choose to select security controls from NIST SP 800-53, but are also free to select from ISACA COBIT 5, ISO/IEC 27001/27002, or other security control catalogs
- NIST CSF Informative Resources refer to certain controls from NIST SP 800-53, but the CSF does not reference the complete set of NIST SP 800-53 controls
- NIST CSF describes its own cybersecurity improvement process that leverages CSF Profiles and Implementation Tiers, but without the rigor of the NIST RMF (e.g., no FIPS 199 System Categorization)

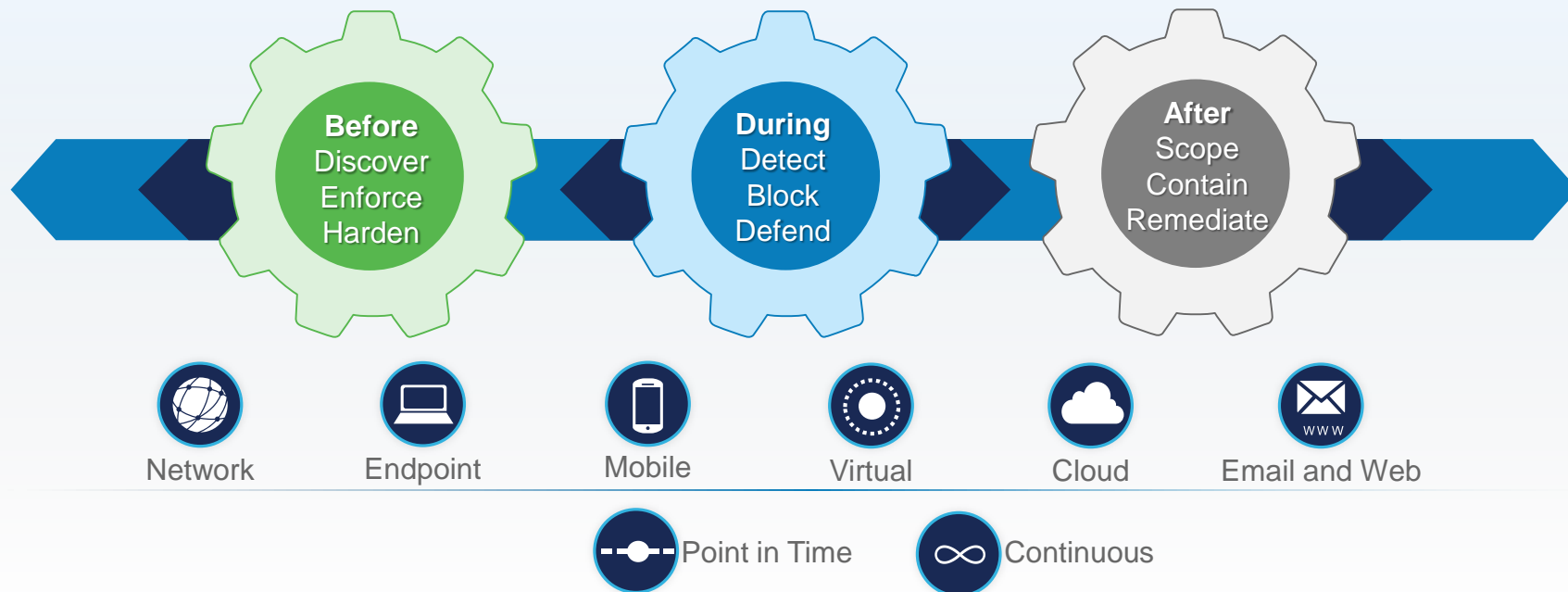




# Cisco Security Strategy

## The Threat-Centric Security Model

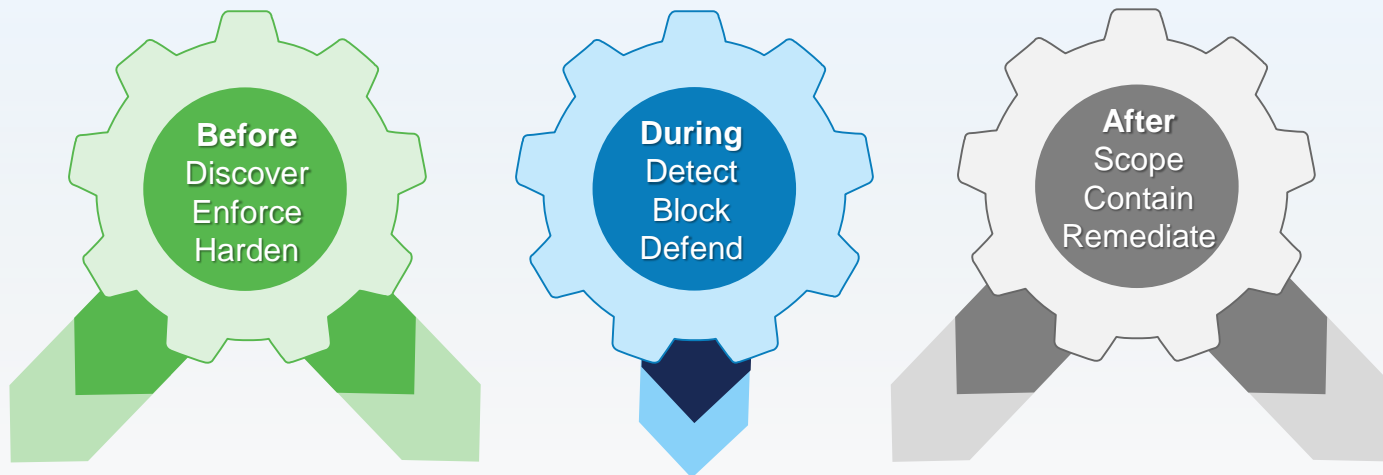
### Attack Continuum



# Cisco Security Strategy

## NIST CSF Alignment

### Attack Continuum



CSF

Identify

Protect

Detect

Respond

Recover

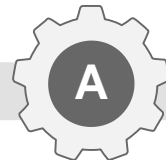
# Cisco Security Products

## NIST CSF Alignment

Technology



		AMP/Threat Grid	Lancome StealthWatch	Cloud Access Security (CAS)	Web/Email Security	Cognitive Threat Analytics (CTA)	OpenDNS	Firepower	Identity Services Engine (ISE)	TrustSec	AnyConnect
ID	Asset Management										
	Business Environment										
	Governance										
	Risk Assessment										
	Risk Mgmt. Strategy										
PR	Access Control										
	Awareness/Training										
	Data Security										
	Info Protection Process										
	Maintenance										
DE	Anomalies and Events										
	Detection Processes										
	Continuous Monitoring										
RS	Response Planning										
	Communications										
	Analysis										
	Mitigation										
	Improvements										
RC	Recovery Planning										
	Improvements										
	Communications										



# Cisco Security Services

## NIST CSF Alignment



		Advisory	Integration	Managed	
ID	Asset Management				
	Business Environment				
	Governance				
	Risk Assessment				
	Risk Mgmt. Strategy				
PR	Access Control				B
	Awareness/Training				
	Data Security				
	Info Protection Process				
	Maintenance				
DE	Protective Technology				D
	Anomalies and Events				
	Continuous Monitoring				
RS	Detection Processes				A
	Response Planning				
	Communications				
	Analysis				
	Mitigation				
RC	Improvements				
	Recovery Planning				
	Communications				



# Conclusion

# Summary

Did we accomplish our goals?

1. TAC 202 ✓ Showed how it relates to NIST SP 800-53
2. About NIST ✓ Discussed who they are and what they do
3. NIST SP 800-53 ✓ Explained how the control catalog works
4. FISMA and NIST RMF ✓ Connected these with Revised TAC 202
5. NIST CSF ✓ Recommended it for cyber risk management

# Call to Action

**1** Learn more about the Texas Cybersecurity Framework:  
<http://dir.texas.gov>



**2** Learn more about NIST cybersecurity best practices:  
<http://csrc.nist.gov>



**3** Learn more about Cisco's threat-centric security:  
<http://www.cisco.com/go/security>



## Thanks for your time today!





**CISCO**

*TOMORROW starts here.*